# OpenID Foundation

2400 Camino Ramon, Suite 375
San Ramon, CA 94583
United States
Telephone: +1 925-275-6639
FAX: +1 925-275-6691


May 19, 2021

Office of Strategy, Policy and Plans
Department of Homeland Security (DHS)
2707 Martin Luther King Jr Ave SE
Washington, DC 20528-0525

Re: Response to the Request for Comments for Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Mobile Driver's Licenses

The OpenID Foundation applauds the choice of ISO/IEC 18013-5 to use OpenID Connect as one of the optional online data transfer modes.

OpenID Connect is a modern identity protocol built on OAuth 2.0 that enables third-party authentication to applications in a standard way and has been deployed and used by hundreds of millions of people since its publication in 2014. OpenID Connect was developed within the OpenID Foundation by over 300 members encompassing 36 countries working together using an open process.

The OpenID Foundation acknowledges that its members have contributed to ISO/IEC 18013-5 in defining how OpenID Connect can be used to retrieve data between the mdoc reader and the issuing authority in a secure and privacy-preserving manner.

The OpenID Foundation is confident that the model adopted in ISO/IEC 18013-5 addresses currently known security and privacy risks when implemented in compliance to the specification. The model is designed to prevent known attacks, such as the authorization code injection attack, redirect URI validation attack, and cross-site scripting by avoiding the implicit flow, redirects, log files and headers, just to name a few restrictions taken.

Mitigating solutions to the known attacks have been documented by industry experts as a Security Best Current Practice specification for OAuth 2.0, a protocol underlying OpenID Connect, to cover new threats based on the practical experiences. The most recent document can be found here: https://datatracker.ietf.org/doc/html/draft-ietf-oauth-security-topics-18.

When developing browser-based applications that use OAuth 2.0, security considerations and best practices have also been detailed in a specification, found here: https://datatracker.ietf.org/doc/html/draft-ietf-oauth-browser-based-apps-08.

The OpenID Foundation would like to highlight its recent work to update Self-Issued OpenID Provider Model, originally defined in OpenID Connect Section 7, which enables End-Users to use OpenID Providers (OPs) that they control. OpenII Connect can meet 18013-5's additional privacy requirements, since using OpenID Connect, the issuing authority sends data directly to the mdoc reader upon receiving the access token from the mdoc. Self-Issued OpenID Provider can meet additional privacy requirements in the upcoming enhancements to ISO/IEC 18013-5 to enable online data transfer directly between the mdoc and the mdoc reader without the mdoc reader contacting the issuing authority.

The Self-Issued OpenID Provider-related submission to the ISO/IEC SC17 JTC1 WG 4 and WG10 is included in the annex to this document.

Finally, the OpenID Foundation would like to mention a work item to standardize how W3C Verifiable Presentations can be transported using OpenID Connect. In scenarios where 18013-5 is being used for identity proofing, device binding, or holder binding capability, this becomes crucial. mdoc holders being able to prove possession of the claims by sending them as W3C Verifiable Presentations, when used in combination with above-mentioned Self-Issued OpenID Provider model, enables tying the presenter of the claim to the legitimate holder of the claim.

Thank you for your consideration.

Regards,

Nat Sakimura

OpenID Foundation Chairman

On behalf of the AB/Connect Working Group of the OpenID Foundation

Annex

# OIDC SIOP (Self-Issued OP) proposal

Contributor: Anthony Nadalin, Kenichi Nakamura, Kristina Yasuda

## Introduction

This contribution is aimed to introduce the OIDC SIOP (self-issuing OIDC provider) model to ISO/IEC 23220 series and ISO/IEC 18013 Part 5.

With a physical driving licence, the issuing authority has no knowledge of who the user is showing their driving licence to. However, the OIDC protocol specified in ISO/IEC 18013-5 requires that the issuing authority (OpenID provider) must know about and communicate with mDL reader. This may violate the user's privacy.

In this OIDC SIOP model, the mobile device runs an OIDC SIOP service along with the mdoc application. When a user wishes to send their identity (and attribute) information to an mdoc reader, they select OIDC SIOP for authentication rather than the issuing authority infrastructure. When an mdoc reader sends an information request to the mdoc holder's OIDC SIOP on the mobile device, the OIDC SIOP requests the mdoc application to present the mdoc. The mdoc application returns ID Token to the mdoc holder's OIDC SIOP. The mdoc holder's OISC SIOP returns it to the mdoc reader. W3C Verifiable Credential data model (i.e., Verifiable Presentation) is also applicable to ID Token. As a result, a user can present identity (and attribute) information to the mdoc reader without sharing any information with the issuing authority.

We wish to contribute,

- To ISO/IEC 23220-1 proposing an additional architecture.
- To ISO/IEC TS 23220-4, proposing a generic OIDC SIOP framework.
- To ISO/IEC 18013-5, proposing OIDC SIOP amendment referencing to ISO/IEC 23220-4 OIDC SIOP framework.

Editor's NOTE Amendment to ISO/IEC 18013-5 or ISO/IEC TS 18013-7?
Editor's NOTE Open items--> Capability exchange

- Disambiguation data (two possibilities)
    - Add the SIOP options to RetrievalOptions with the following CDDL structure:

```
RetrievalOptions = WifiOptions / BleOptions / NfcOptions / ServerUrlOptions / OidcSiopOptions

OidcSiopOptions = (

      0: tstr ; URL of the verifier server

      ?1: boolean : OIDC SIOP Client support
```

```
}
```

- Add the SIOP capability to ServerUrlOptions with the following CDDL structure

```
ServerUrlOptions = {
      0: tstr ; URL of the verifier server
      ?1: unit ; 1 OIDC SIOP Client support
                 2 RESTAPI Verifiable presentation mapping
}
```

## Normative references


RFC 8252, *OAuth 2.0 for Native Apps*

OpenID foundation, *OpenID Connect Core 1.0 incorporating errata set 1*

https://openid.net/specs/openid-connect-core-1_0.html

OpenID foundation, *OpenID Connect Discovery 1.0 incorporating errata set 1,*

https://openid.net/specs/openid-connect-discovery-1_0.html


## Proposal to ISO/IEC 23220-1

*P11, 3.31,*

Add the following definition after 3.31:

3,32 remote user storage

remote storage service that is used by a user with access authorization by the user being required if someone wishes to retrieve a data from this storage

*P29, 10.2,*

Add the following paragraphs and Figure after Figure 17 and replace the last two paragraphs with;

A user may use a Remote User Storage Service instead of Identity and Attribute Provider Service as described in Figure 18. In this case, a user transmits user attributes via mobile eID-App and also allows a Service Provider to access to the user's Remote User Storage. Then a Service Provider may access the user's Remote User Storage and retrieve additional user attributes (see interface PR-7 in Figure 18). The interface PR-4 (see Figure 17) may also be supported in this architecture. This prevents the Identity and Attribute Provider Service from knowing the access log for the user's attributes.

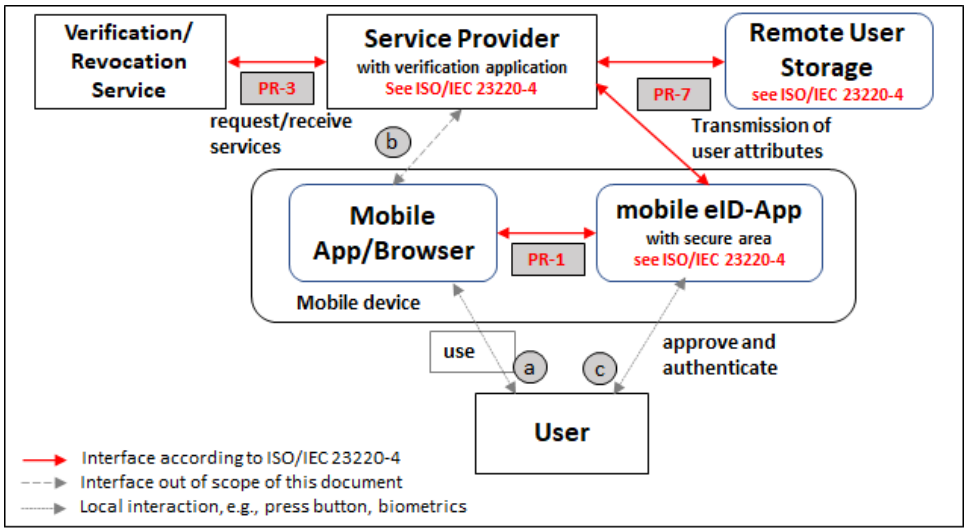


Figure 18 Remote identification system architecture with remote user storage

This system architecture includes the Verification Application, the Identity or Attribute Provider and mobile eID-App with interfaces PR-1, PR-3, PR4, PR-5, PR-6 and PR-7 in Figure 16 and Figure 17.

The verification and revocation infrastructure service of this system architecture may be operated by a separate service or by one single service and includes relation PR-3 in Figure 16 and Figure 17.

# Proposal to ISO/IEC TS 23220-4

### 7.1.3.4 OIDC SIOP (Self-Issued Open ID Provider)

#### 7.1.3.4.1 OIDC SIOP model

OIDC SIOP is an extension of OpenID Connect (See 7.2.1) to allow mdoc holder to use OpenID Providers (OPs) that they control and present mdoc data directly to mdoc reader as a device retrieval method and it prevents the issuing authority from knowing usage information of mdoc data via communication with the mdoc reader. OIDC SIOP is specified in OpenID foundation, OpenID Connect Core 1.0 incorporating errata set 1, Section 7.

Figure X describes the OIDC SIOP system architecture.

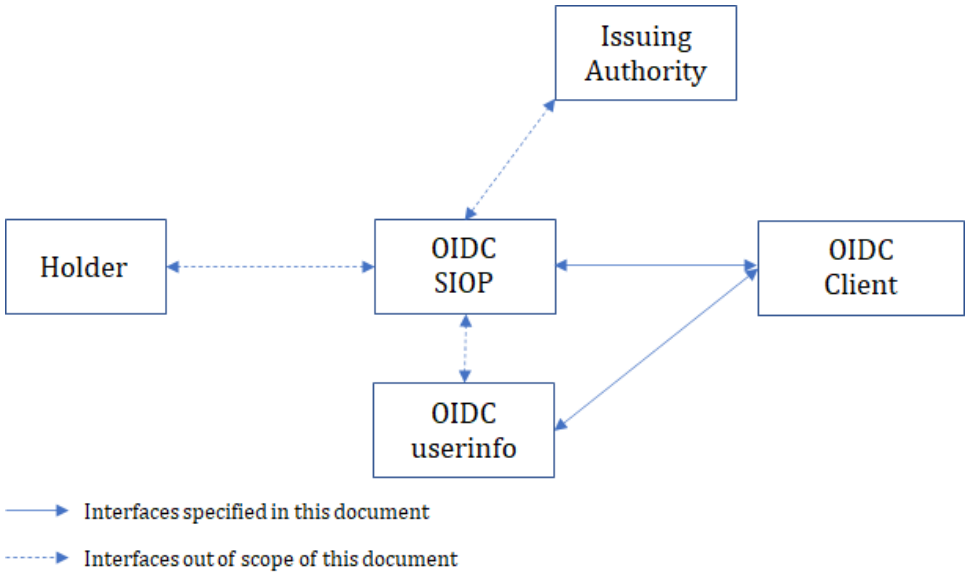


Figure X OIDC SIOP system architecture

This document specifies interface between OIDC SIOP and OIDC Client that is used for data retrieval. Additionally, the use of OIDC UserInfo endpoint is also specified. The discovery of the location of the OIDC UserInfo endpoint is out of scope of this document.

The interface between the holder and OIDC SIOP is required for user authentication for the mdoc data retrieval service and the requirements for this interface are out of scope of this standard. The interface between the Issuing Authority and OIDC SIOP is also out of scope. OIDC SIOP is applicable to remote identification system architecture (See ISO/IEC 23220-1, Clause 10). OIDC SIOP is supported by mobile eID-app and OIDC Client is supported by Service Provider (See ISO/IEC 23220-1, Clause 10, Figure 14). In this document, the OIDC SIOP may support the UserInfo endpoint and provides additional information, which includes claims not included in ID Token.

Editor's note We need to propose to add "remote user storage" entity in ISO/IEC 23220-1 for supporting the UserInfo endpoint.

The protocol between OIDC SIOP and OIDC Relying Party consists of the following four steps:

- SIOP discovery (See 7.1.3.4.2)
- SIOP registration (See 7.1.3.4.3)
- Authorization Request and ID Token retrieval (See 7.1.3.4.4)
- ID Token validation (See 7.1.3.4.5)

#### 7.1.3.4.2 SIOP discovery

For SIOP discovery, OpenID connect dynamic discovery is not applicable and a static configuration may be used. If static configuration is not used, the value of the configuration parameters should be negotiated between OIDC SIOP and OIDC Client in advance.

The value of the "id_token_signing_alg_values_supported" parameter shall be any subset of ”ES256”, “ES384”, “ES512”, and ”EdDSA”, as specified in ISO/IEC 18013-5:2021, 9.1.2.4. The value of "request_object_signing_alg_values_supported" shall be any subset of ”ES256”, “ES384”, “ES512”, and ”EdDSA”, as specified in ISO/IEC 18013-5:2021, 9.1.3.6.

The description of the URL that is used to invoke SIOP may be custom URL schema or universal URLs. If SIOP supports multiple mdocs, then OIDC SIOP and OIDC Client shall negotiate a mechanism to invoke a particular mdoc in advance.

The static configuration shall support URL of UserInfo endpoint, if OIDC SIOP support UserInfo endpoint.

#### 7.1.3.4.3 SIOP registration

The OIDC registration process is required for SIOP. OIDC Client may use the “registration” element in the Authorization Request, as specified in OpenID Connect Core 1.0 incorporating errata set 1, 7.2.1.

#### 7.1.3.4.4 Authorization request and ID Token retrieval

OIDC Client sends the Authorization Request to the Authorization endpoint of SIOP, as specified in OpenID Connect Core 1.0 incorporating errata set 1, 7.3.

If OIDC Client indicates the intent to store the data at the data element level, then the Boolean field “intent to store” shall be mapped to each claim.

EXAMPLE

```
{
"claims": {
  "id_token": {
    "verified_claims": {
      "claims": {
```

```
        "given_name": {
          "intent_to_store": true
         },
        "family_name": {
           "intent_to_store": true
         },
        "birthdate": null,
        "nationality": null,
        "address": null
      }
    }
  }
}
```

SIOP sends the Authorization Response to the OIDC Client as specified in OpenID Connect Core 1.0 incorporating errata set 1, 7.4. An ID Token shall be returned if OIDC Client sends a SIOP Authorization message.

It should be noted that the value of iss (issuer) claim in SIOP response is https://self-issued.me and it does not indicate the issuer of the mdoc.

The following example shows the claims of the JWT:

```
{
  "iss": "https://self-issued.me",
  "iat": 1611543618,
  "exp": 1611543918,
  "aud": "https://utopiadot.gov/resources",
  "sub": "1",
  "doctype": "org.iso.18013.5.1.mDL",
  "given_name": "(CBOR encoded given name)",
  "family_name": "(CBOR encoded family name)",
  "birth_date": "1971-09-01",
  "MSO": "{CBOR encoded MSO blob}"
}
```

The device authentication key as specified in ISO/IEC 18013-5, 9.1.3.4 shall be used for signing the ID Token. A JWK Thumbprink shall be used as the subject identifier for SIOP.

The OIDC SIOP may send an Access token in addition to an ID Token.

NOTE The current OpenID Connect specification does not specify the use of an Access token by SIOP.

If not all the requested claims are included in ID Token, such claims can be provided via a UserInfo endpoint hosted by the user. An access token can be used to access to the UserInfo endpoint. The access token enables retrieving claims from the UserInfo endpoint.

#### 7.1.3.4.5 ID Token validation

The mdoc reader validates the ID Token as specified in OpenID Connect Core 1.0 incorporating errata set 1, 7.5.

#### 7.1.3.4.6 Access to UserInfo Endpoint

OIDC Client may send UserInfo request to UserInfo endpoint. The use of UserInfo endpoint is specified in OpenID Connect Core 1.0 incorporating errata set 1, 5.3.